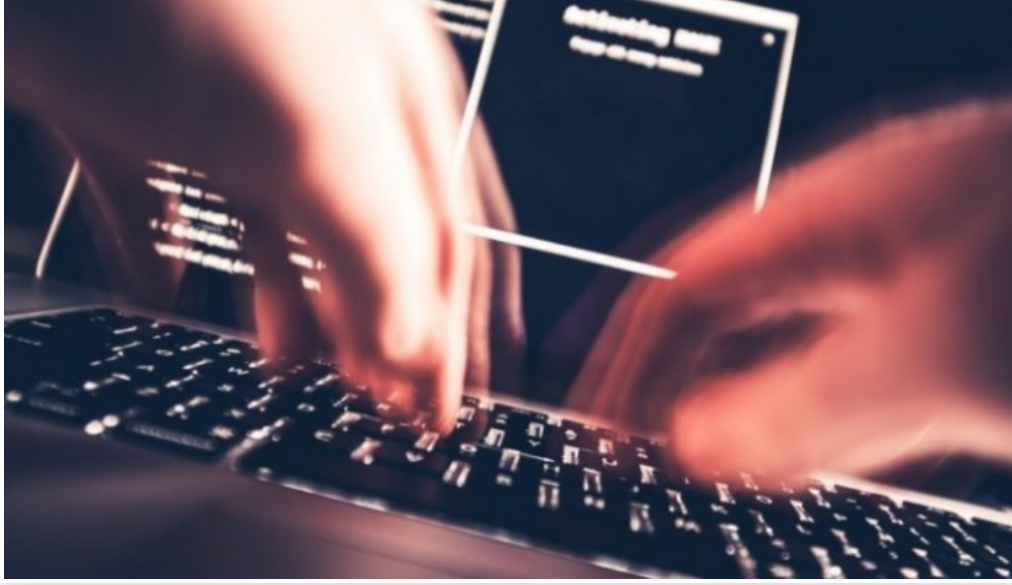


سيمانتيك: قرصنة يهاجمون شركات الطاقة الأمريكية والأوروبية



الأربعاء 6 سبتمبر 2017 07:09 م

استهدفت مجموعة من القرصنة شركات الطاقة الأمريكية والأوروبية في حملة تجسس إلكتروني نجحت في بعض الحالات في كسر الأنظمة الأساسية التي تسيطر على عمليات الشركات بهدف تخريب شبكات الكهرباء الوطنية، وذلك وفقاً لما ذكره الباحثون في شركة الأمن السيبراني سيمانتيك Symantec، الذين ذكروا في تقرير تم نشره اليوم الأربعاء انه تم استعمال حملات بريدية ضارة للدخول إلى المنظمات في الولايات المتحدة وتركيا وسويسرا ودول أخرى محتملة

وقال اريك شين الباحث الامني السيبراني في شركة سيمانتيك ان الهجمات السيبرانية قد بدأت في اواخر عام 2015، لكنها ازدادت تواتراً في شهر ابريل / نيسان من هذا العام، وانها على الأرجح من عمل حكومة اجنبية وتحمل السمات المميزة لمجموعة القرصنة المعروفة باسم "اليغسوب" Dragonfly، ويوضح التقرير أن الشركات الصناعية، بما في ذلك مقدمي الطاقة والمرافق الاخرى، عرضة للهجمات السيبرانية التي يمكن الاستفادة منها لأغراض تدميرية في حالة نشوب نزاع جيوسياسي كبير

وقد حذرت الحكومة الأمريكية في شهر يونيو/حزيران الماضي الشركات الصناعية من حملات القرصنة التي تستهدف قطاع الطاقة النووية، قائلة في إنذارها أن القرصنة أرسلو رسائل تصيد احتيالي للحصول على أوراق الاعتماد من أجل الوصول إلى الشبكات المستهدفة، وقال شيان انه يعتقد ان تنبيه الحكومة مرتبط بنفس الحملة التي تتبعها شركة سيمانتيك، وأن عشرات الشركات قد استهدفت وأن عدد قليل منهم، بما في ذلك الولايات المتحدة، قد تعرض للخطر على المستوى التشغيلي

وقال شين ان هذا المستوى من الوصول يعني ان الدافع هو الخطوة الوحيدة الباقية التي تحول دون تخريب شبكة الكهرباء، ومع ذلك، يلقي باحثون آخرون بعض الشكوك حول النتائج، ويوضح التقرير انه طالما أن الهجمات ما زالت في مستوى بعيد عن القدرة على إطفاء الإضاءة فليس هناك حاجة للتهويل والاذار

ورغم أن سيمانتيك لم تذكر روسيا في تقريرها إلا انها أشارت إلى أن المهاجمين استعملوا سلاسل تعليمات برمجية باللغة الروسية، بينما تستعمل تعليمات برمجية أخرى اللغة الفرنسية، مما يشير إلى أن المهاجمين يحاولون جعل من الصعوبة بمكان التعرف عليهم

تجدد الإشارة إلى أن جماعة Dragonfly كانت تعمل بشكل نشيط في السابق، بين عامي 2011 و2014، وقد قللت من نشاطها بعد قيام العديد من شركات الأبحاث الأمنية بنشر أبحاث تسلط الضوء على هجماتها، ويعتقد على نطاق واسع أن المجموعة المعروفة أيضاً باسم "الدب النشط" Energetic Bear أو "كوالا" Koala، كانت مرتبطة بالحكومة الروسية، وانها قامت بزرع أبواب خلفية في أنظمة التحكم الصناعي لمحطات توليد الطاقة في جميع أنحاء الولايات المتحدة وأوروبا